UEFI-2026

UEFI-2026 - Readiness

TITEL	UEFI-2026
AUTOR	Docusnap Consulting
DATUM	18.09.2025
VERSION	1.0 | gültig ab 26.08.2025

Die Weitergabe, sowie Vervielfältigung dieser Unterlage, auch von Teilen, Verwertung und Mitteilung ihres Inhaltes ist nicht gestattet, soweit nicht ausdrücklich durch die Docusnap GmbH zugestanden. Zuwiderhandlung verpflichtet zu Schadenersatz. Alle Rechte vorbehalten.

This document contains proprietary information and may not be reproduced in any form or parts whatsoever, nor may be used by or its contents divulged to third parties without written permission of Docusnap GmbH. All rights reserved.

INHALTSVERZEICHNIS

1. Einleitung 4
1.1 Bezug aktueller Zertifikate 5
1.2 Einschränkungen ohne Telemetrie 6
2. Voraussetzungen 7
3. Analyse mit Docusnap 8
4. Hinweis 9

1. Einleitung

Im Jahr 2026 stehen Millionen von Systemen weltweit vor einem sicherheitskritischen Problem: Die bislang genutzten Microsoft-Zertifikate für **UEFI Secure Boot** laufen ab.

Secure Boot ist eine zentrale Sicherheitsmechanik, die verhindert, dass beim Start des Rechners manipulierte oder unsignierte Software geladen wird. Mit dem Ablauf der Zertifikate im **Juni und Oktober 2026** verlieren viele Geräte die Fähigkeit, neue Firmware- oder Betriebssystem-Updates als vertrauenswürdig einzustufen.

Betroffene Systeme:

- klassische Windows-PCs und -Server
- virtuelle Maschinen
- Dual-Boot-Systeme mit Linux oder macOS

Ohne rechtzeitige Maßnahmen – wie die Installation neuer Zertifikate oder notwendiger Firmware-Updates – droht im schlimmsten Fall, dass Systeme **nicht mehr starten** oder **dauerhaft Sicherheitslücken** offenbleiben.

Docusnap ermöglicht es, zu erkennen, ob noch alte Zertifikate aktiv sind oder ob bereits ein Austausch auf die neuen Zertifikate erfolgt ist. Administratoren erhalten so eine verlässliche Grundlage, um Handlungsbedarf zu erkennen und Maßnahmen gezielt zu planen.

1.1 Bezug aktueller Zertifikate

Über Windows Update (automatisiert)

- Systeme, die regulär Windows Updates beziehen und Telemetrie senden, werden automatisch in das *Managed Certificate Update* aufgenommen.
- Ab Juli 2025 werden vorbereitende Updates verteilt (z. B. KB5064489).
- Neue Zertifikate (KEK 2K CA 2023, UEFI CA 2023, Option ROM UEFI CA 2023) werden über den Update-Mechanismus in den UEFI-Zertifikatsspeicher eingetragen.

Über Firmware-/BIOS-Updates vom OEM

- Hersteller wie HP, Dell, Lenovo liefern die Zertifikate über BIOS-/UEFI-Updates.
- Diese müssen manuell oder über Hersteller-Management-Tools eingespielt werden, falls Windows Update blockiert oder nicht genutzt wird.

1.2 Einschränkungen ohne Telemetrie

Microsoft weist ausdrücklich darauf hin: **Ohne Telemetrie** werden Geräte nicht automatisch in die Rollout-Gruppe aufgenommen.

Konsequenz:

- Systeme ohne Telemetrie erhalten keine neuen Zertifikate über Windows Update.
- Sie behalten die alten **2011er-Zertifikate** und laufen damit direkt in das *UEFI-2026 Problem*.

Auswirkungen:

- **Ab Juni 2026:** Ablauf von KEK und UEFI CA 2011 → keine Installation neuer Boot-Treiber oder Firmwarekomponenten mehr möglich.
- **Ab Oktober 2026:** Ablauf des Windows Production PCA 2011 → keine Bootloader-Updates mehr möglich.

Folge: Systeme können unsicher werden (z. B. kein Schutz vor Bootkits wie **BlackLotus**) oder im Extremfall nicht mehr starten.

2. Voraussetzungen

Bei der Windows-Inventarisierung müssen auch die Trusted-Zertifikate ausgelesen werden. Standardmäßig sind diese in der Komponenten-Auswahl jedoch nicht aktiviert. Das Auslesen der Zertifikate erfordert administrative Berechtigungen auf dem System.

3. Analyse mit Docusnap

Zur Überprüfung der **UEFI-2026 Readiness** prüft Docusnap die Existenz folgender Zertifikate:

- CN=Microsoft Corporation KEK 2K CA 2023
  Thumbprint: 459AB6FB5E284D272D5E3E6ABC8ED663829D632B
- CN=Microsoft Option ROM UEFI CA 2023
  Thumbprint: 3FB39E2B8BD183BF9E4594E72183CA60AFCD4277
- CN=Microsoft UEFI CA 2023
  Thumbprint: B5EEB4A6706048073F0ED296E7F580A790B59EAA

Die Identifikation erfolgt über die Thumbprints.

Auswertung in Docusnap

Über den Bericht **UEFI 2026 Readiness** (Pfad: *Firma → Infrastruktur → Domäne → Berichte → Infrastruktur HW → UEFI 2026 Readiness*) und ein entsprechendes **Connect-Paket** (UEFI 2026 Readiness) lässt sich feststellen, ob Geräte bereits „UEFI 2026 Ready" sind.

Statusauswertung

- **Ja** – Zertifikate mit den o. g. Thumbprints vorhanden
- **Nein** – Zertifikate fehlen
- **Nicht ermittelbar** – Zertifikate konnten nicht ausgelesen werden

4. Hinweis

Docusnap kann keine Handlungsempfehlungen geben, wenn die erforderlichen Zertifikate fehlen. Die Lösung zeigt ausschließlich, ob ein Gerät bereits über die neuen Zertifikate verfügt und damit „UEFI 2026 Ready“ ist. Für weiterführende Informationen oder notwendige Maßnahmen müssen Administratoren die Hinweise des jeweiligen Herstellers einholen.

Weiterführende Informationen:
Microsoft Tech Community Blog – Act now: Secure Boot certificates expire in June 2026

VERSIONSHISTORIE

Datum	Beschreibung
26.08.2025	Dokument erstellt

Docusnap

© Docusnap GmbH - www.docusnap.com